

Solid–State Drive (SSD) Structure & Forensics

Second Edition

SSD Forensics နဲ့ပတ်သတ်ပြီး ရေးထားသမျှ
Blog Post Collection PDF ပါ။

Aung Zaw Myo
www.forensicsmyanmar.com

SSD တွေက HDD နဲ့မတူတဲ့အချက်ကတော့ Flash Translation Layer (FTL)မှာ Garbage collection နဲ့ Ware-Leveling တို့ကြောင့်ဖြစ်ပါတယ်။ FTL က Logical Block နဲ့ Physical Block ကို ချိတ်ဆက်ပေးတာဖြစ်ပါတယ်။ SSD တင်တဲ့ထား Operation System ကနေ Physical File နေရာတွေကို Track လုပ်မထားပါဘူး။ HDD နဲ့ကွဲပြားချက်ဖြစ်ပါတယ်။

Garbage Collection (GC)

HDD မှာလို Data တစ်ခုသိမ်းမယ်ဆိုရင် ရှိနေပြီးသား Data ပေါ်မှာ SSD Nand Flash က မသိမ်းနိုင် OverWrite မလုပ်နိုင်ပါဘူး။ Data သိမ်းမယ်ဆိုရင် Block ကို Erase လုပ် ပြီးမှ သိမ်းရပါတယ်။ မဖျက်ခင် Block ထဲက Data ကို အခြား Block ပေါ် ပြောင်းတာလဲရှိပါတယ်။ အခုလို Bock ကို Erase လုပ် Block တွေကို ပြန်နေရာချတာကို Garbage Collection လို့ခေါ်ပါတယ်။ Garbage collection က SSD ထဲကနေ မလိုအပ်တဲ့ data တွေဖယ်ထုတ်ပြီး နောက်ထပ် data တွေသိမ်းလို့ရအောင် ပြုလုပ်ပေးပါတယ်။data သိမ်းဆည်းဖို့ အမှန်တစ်ကယ် Page တစ်ခုသာ လိုအပ်ပေမဲ့ Garbage collection ပြုလုပ်တဲ့အခါ Block တစ်ခုလုံးကို ဖျက်ပါတယ်။ Block ထဲမှာ data တွေရှိရင်လဲ အခြား Page,Block ကို အလိုအလျှောက်ပြောင်းလဲပေးပါတယ်။

Photo (1) အရဆိုရင် Block A ထဲက Page-1 မှာ data save ချင်တယ်- ဒါပေမဲ့ ကျန်တဲ့ Page-2,3,4 မှာ တစ်ကယ့် data တွေကျန်နေသေးတယ်ဆိုရင် Page-2,3,4 က Data တွေက Block-B ကိုရောက်သွားပါတယ်။ Block-B မှာ Block-A ကနေ Page 3 ခုသာပြောင်းသွားတဲ့အတွက် Block-B မှာ Page တစ်ခုလွတ်နေပါတယ်။ လွတ်နေတဲ့ Page မှာ Zero တွေအဖြစ်ရှိပါတယ်။ (AFF4 Image လုပ်တဲ့နေရာမှာ အခုလိုဖြစ်တဲ့ Zero တွေကို ချန်လုပ်ပြီး Image လုပ်နိုင်တဲ့အတွက် ပိုမြန်တာလဲပါပါတယ်)

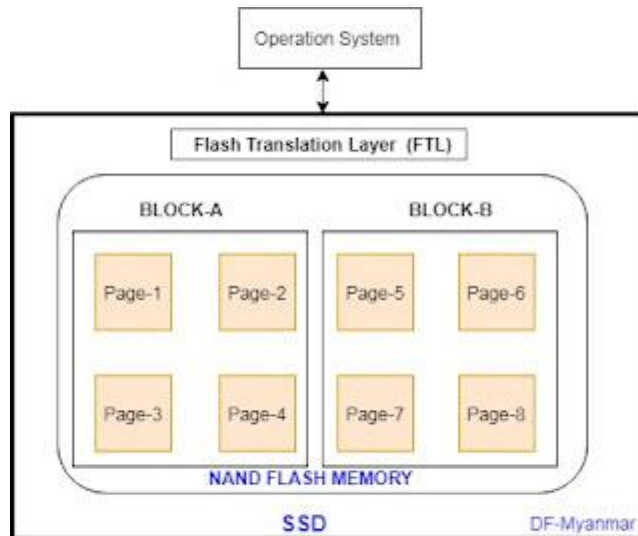


Photo (1)

TRIM

TRIM-enabled လုပ်ထားတဲ့ SSD drives က garbage collection (GC) ကြောင့် ဖျက်လိုက်တဲ့ Data တွေကိုပြန်ရနိုင်ဖို့ခက်ခဲပါတယ်။ TRIM ဆိုတာက ဥပမာ အချက်အလက်တစ်ခုကို ဖျက်လိုက်မယ်ဆိုရင် SSD ထဲမှာ အပြီးဖျက်လိုက်မယ်ဆိုပြီး SSD Controller က နေတစ်ဆင့် Data သိမ်းထားတဲ့ Page Or Block ထဲကို ဖျက်ခိုင်းလိုက်တာပါ။ TRIM က ကွန်ပျူတာ ပါဝါ ပိတ်ထားလိုက်ရင် လုပ်နေတဲ့ အလုပ်ကို ခနရပ်ထားပါတယ်။ ဒါပေမဲ့ ကွန်ပျူတာ ပါဝါ ပြန်ဖွင့်တာနဲ့ ပြန်အလုပ်လုပ်ပါတယ်။ ဘာလို့လဲဆိုရင် လုပ်နေတဲ့ အလုပ်ကို SSD Controller ထဲမှာ သိမ်းထားလို့ဖြစ်ပါတယ်။ Trim က RAID configuration, NAS configuration, window 7 နှင့် နောက်ပိုင်း ပြီးရင် SSD ကို External Hard Disk အဖြစ်သုံးတဲ့နေရာတွေမှာ မပြုလုပ်နိုင်ပါဘူး။ Win 8, 8.1 , Win 10,Mac OS X, Mac book with Windows တွေမှာသာအသုံးပြုနိုင်ပါတယ်။ Recyclebin ကို Delete လုပ်တာနဲ့ SSD ရဲ့ Block တွေမှာ တစ်ခါတည်းဖျက်လိုက်ပါတယ်။ နောက်ထပ် Data တွေ Save နိုင်အောင်ဖြစ်ပါတယ်။ Flash Translation Layer မှာပါဝင်တဲ့ Function တွေကြောင့် SSD ကို Forensics Image ပြုလုပ်ပြီး Hash Methdology (MD5,SHA) ပြုလုပ်ရင် Hash Value မတူညီနိုင်ပါဘူး

Self Corrosion

Trim က ကွန်ပျူတာကနေ SSD ကိုဖြုတ်လိုက်ရင်လဲ SSD ကိုပါဝါပေးတာနဲ့ အလုပ်လုပ်နေတာဖြစ်ပါတယ်။

Write-Blocking Imaging Device ကိုကြားခံအသုံးပြုရင်လဲ ဆက်ပြီး အလုပ်လုပ်နေမှာ ဖြစ်ပါတယ်။ Trim ကို ပိတ်ဖို့ ရှောင်လွှဲဖို့ ယနေ့အထိ ခက်ခဲနေပါသေးတယ်။ User ကနေ Trim enable လုပ်ထားပြီး data တစ်ခုကို ဖျက်မယ် Format လုပ်မယ် Wipe လုပ်မယ်ဆိုတဲ့အပေါ်မူတည်ပြီး Window - SSD Controller ကနေတစ်ဆင့် အလုပ်လုပ်တာဖြစ်ပါတယ်။ SSD ရဲ့ hardware level မှာ အလုပ်လုပ်တာဖြစ်ပါတယ်။ ဒီလို နောက်ကွယ်မှာ Garbage Collection (GC) အလုပ်လုပ်နေတာကိုSelf Corrosion ပြုလုပ်တယ်လို့လဲခေါ်ပါတယ်။

Over Provisioning

SSD ရဲ့ Performance ကောင်းဖို့ လုပ်တာဖြစ်ပါတယ်။ Garbage Collection, Wear-Leveling, Bad Block Management လုပ်တာတွေကို ပိုမိုကောင်းမွန်စေဖို့ ပြုလုပ်တာဖြစ်ပါတယ်။ SSD မှာ Data သိမ်းဆည်းရင် Page က 4KB ရှိပြီး Block တစ်ခုမှာ 128 Pages ရှိပါတယ် Block တစ်ခုမှာ 512 KB ရှိပါတယ်။။ Write လုပ်လုပ် Erase လုပ်လုပ် Block တစ်ခုလုံးကို လုပ်တာဖြစ်ပါတယ်။ Controller Firmware နဲ့ Failed Block Replacement အတွက် SSD Storage မှာ သီးသန့်ချန်ထားတဲ့ Free Space Block တွေရှိပါတ်။ SSD အမျိုးအစားအပေါ် မူတည်ပြီး Free Space Block အရေအတွက် ကွဲပြားပါတယ်။

Wear leveling

SSD ရဲ့ Block တွေမှာ Erase\Write Cycles သတ်မှတ်ချက်ရှိပါတယ်။ ဒါကြောင့် Wear leveling က SSD ရဲ့ Life ကို ကြာမြင့်စေဖို့ ပြုလုပ်ပေးပါတယ်။ Wear leveling ကို SSD Controller ကနေပဲပြုလုပ်တာဖြစ်ပါတယ်။ ဘယ် Block က

Erase\Write လုပ်တာ အကြိမ်ဘယ်လောက်ရှိပြီဆိုတာကို စောင့်ကြည့်နေပါတယ်။ စောင့်ကြည့်ပြီးရင် Data တစ်ခုကို SSD ပေါ်မှာ သိမ်းမယ်ဆိုရင် Erase\Write အနည်းဆုံး Block ပေါ်မှာ သိမ်းဆည်းပါတယ်။

Dynamic wear leveling နဲ့ Static wear leveling ဆိုပြီး ၂ မျိုးရှိပါတယ်။ Dynamic wear leveling က Erase\Write အနည်းဆုံးဖြစ်တဲ့ Block တွေကို မှတ်သား ထားပြီး Data သိမ်းမဲ့ Block ကိုရွေးပါတယ်။ Static wear leveling ကတော့ Data သိမ်းမဲ့ Block က Erase\Write အနည်းဆုံးဖြစ် မဖြစ်ကြည့်ပါတယ်။ လိုအပ်ရင် Block ကိုဖျက်ပါတယ်။ မဖျက်ခင် Block ထဲမှာ ရှိနေတဲ့ Data ကို Block နောက်တစ်ခုမှာ Data ကိုပြောင်းပြီး သိမ်းလိုက်ပါတယ်။ နောက် Block ထဲကို data သိမ်းလိုက်ပြီးရင် Block ကို ဖျက်လိုက်ပါတယ်။ Block က Empty ဖြစ်သွား ပြီးဆိုတော့မှာ Data ကို သိမ်းတာဖြစ်ပါတယ်။ Garbage Collection (GC) ပြုလုပ်နေချိန်မှာ Wear Leveling ကလဲ အလုပ်လုပ်နေပါတယ်။

TRIM

TRIM Enable ပြုလုပ်ထားရင် စစ်ဆေးသူက ဖျက်လိုက်တဲ့ Data တွေကို ရဖို့မလွယ်ကူနိုင်ပါ။ SSD Controller ကနေ ပြုလုပ်တာဖြစ်တာကြောင့် SSD ကို Power ပေးတာနဲ့ နောက်ကွယ်မှာ ဆက်လက်ပြုလုပ်နေမှာဖြစ်ပါတယ်။ Trim က SSD တစ်ခုလုံးကို ဖျက်ဖို့ မိနစ်ပိုင်း စက္ကန့်ပိုင်းသာ အချိန်ယူပါတယ်။

User -1

SSD ထဲမှာရှိတဲ့ File and Folder တွေကိုအကုန်ဖျက်လိုက်တယ်။ ဖျက်ပြီးတဲ့ နောက်ပိုင်း မည်သည့် Data မှ SSD ထဲကို မထည့်။ နာရီပိုင်း အတွင်း SSD ကို Disk Forensics Tools Or Recovery Software နဲ့ Data တွေကို ပြန်ယူတယ်။ ရာနှုန်းတော်တော်များများသော Data တွေ ပြန်ပေါ်လာတယ်။ ဒါပေမဲ့ Recovery ပြန်ယူတဲ့အခါ File တွေက မရတော့ဘူး။ File က Zero တွေပဲ ဖြစ်နေတယ်။

User -2

SSD ထဲမှာရှိတဲ့ File and Folderတွေကို အကုန်ဖျက်လိုက်တယ်။ ဖျက်ပြီးတဲ့နောက်ပိုင်း မည်သည့် Data မှ SSD ထဲကို မထည့်။ နာရီပိုင်းအတွင်း SSD ကို Disk Forensics Tools Or Recovery Software နဲ့ Data တွေကို ပြန်ယူတယ်။ 80 ရာနှုန်း Data တွေပြန်ရတယ်။ ဘာလို့လဲဆိုရင် SSD အမျိုးအစားအပေါ်မူတည်ပြီး Trim 2 မျိုးကွဲသွားလို့ဖြစ်ပါတယ်။ Android Version 4.3 ကနေစပြီး Trim က Support ပေးပါတယ်။ Live Triming Support ပေးတဲ့သဘောပါ။ Version အဟောင်းတွေမှာတော့ Live Trimming Support မပေးပါဘူး။ Device Power Off တဲ့အချိန်မှသာ Linux မှာ Unused Block တွေကို Cleaning လုပ်တဲ့ Fstram ကြောင့် Trim ကအလုပ်လုပ်ပါတယ်။ဒါကြောင့် Digital Devices သိမ်းဆည်းနည်း Guide Line တွေမှာ Phone ကို Power Off ဆိုရင် Off တဲ့အနေအထားနဲ့ သိမ်း။ Power On နေရင် Power On တဲ့ အနေအထားနဲ့ သိမ်းလို့ ပြောကြတာဖြစ်ပါတယ်။

Wear Leveling

Wear Leveling ကြောင့် ပထမ အချက်က SSD မှာ File,Data,Folder တွေကို Hash Value ယူရတာ တစ်ကြိမ်နဲ့ တစ်ကြိမ်မတူညီနိုင်ပါ။ဒုတိယ အချက်က Forensically Recovery ပြုလုပ်ဖို့ ခက်ခဲတာ ရှာဖွေဖို့ခက်ခဲတာဖြစ်ပါတယ်။

Compressing Controller

SSD ထုတ်လုပ်တဲ့ Company တွေက Controller ကနေ Encryption ပြုလုပ်ထားတဲ့ အတွက် SSD မှာရှိတဲ့ data သိမ်းတဲ့ Flash တွေကိုခွာပြီး စစ်ဆေးမယ်ဆိုရင် Company ကိုပြန်ပို့ရမှာ ဖြစ်ပါတယ်။ (Chip off) Trim ကိုကျော်ဖို့ သုံးတာဖြစ်ပါတယ်။

Secure Erase

Wiping ပြုလုပ်ဖို့ HDD မှာ နာရီပိုင်းအချိန်ယူရပေမဲ့ SSD မှာတော့ မိနစ်ပိုင်းသာ ကြာပါတယ်။

အချို့သော SSD နဲ့ ချိတ်ဆက်မဲ့ interface တွေက အတွင်းပိုင်း အထိ အချက်အလက် တွေ မဖတ်နိုင်ပါဘူး။

SSD ရဲ့ အတွင်းပိုင်း ဖွဲ့စည်းပုံက HDD ထက်ရှုပ်ထွေးပါတယ်။

SSD အတွက် သတ်မှတ်ထားတဲ့ စံသတ်မှတ်ချက်မရှိသေးပါဘူး။

Carving နဲ့ free space analysis ပြုလုပ်ဖို့ခက်ခဲပါတယ်။

SSD မှာ Data တစ်ခုကို Write လုပ်မယ်ဆိုရင် Page/Block(Group Of Pages) တွေမှာ Write လုပ်ပါတယ်။ ဖျက်မယ်ဆိုရင် Block တစ်ခုလုံးကို ဖျက်ပါတယ်။ ဒါကို SSD Controller ကနေပဲ ထိန်းချုပ်ပြီးလုပ်ဆောင်ပါတယ်။

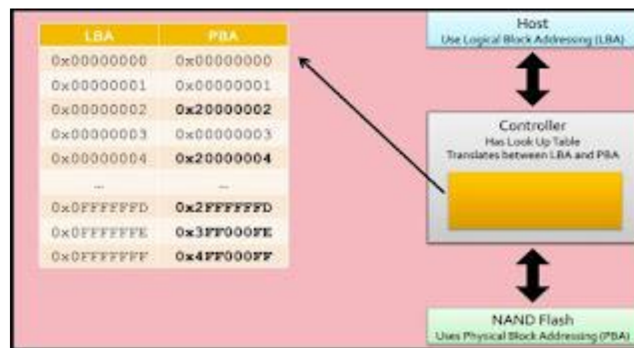
ဒါကြောင့် SSD တပ်ထားမယ်ဆိုရင် Host Operation System က Data ရှိတဲ့ တစ်ကယ့် Physical Block Area နေရာတွေကို မသိပါဘူး။ Data တစ်ခုကိုလိုချင်ရင် ရှာချင်ရင် Host Operation System က LogicalBlock Address ကိုညွှန်းပါတယ်။

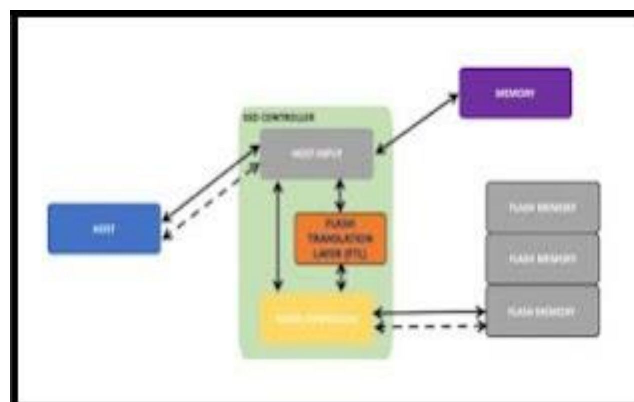
Logical Block Address ကနေ Physical Block Address ရှိတဲ့နေရာကို SSD controller ကနေညွှန်ပြပေးပါတယ်။

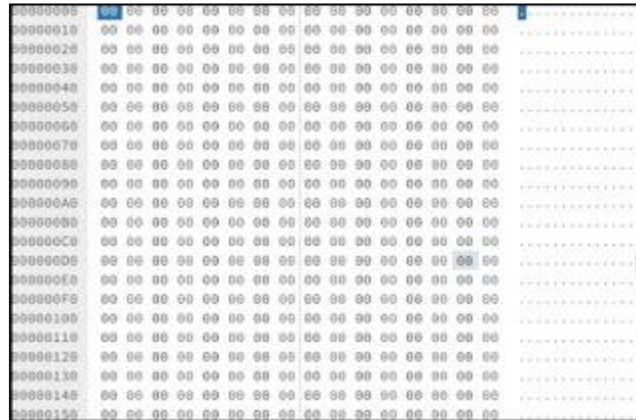
Wear Leveling, Garbage Collection စတာ တွေကိုတော့ SSD controller ထဲက Flash Translation Layer (FTL)ကနေပြုလုပ်ပါတယ်။ အခုလက်ရှိသုံးနေတဲ့ Forensics Tools ၉၉ ရာခိုင်နှုန်း က Flash Translation Layer (FTL) အထိ မဖတ်နိုင်ပါဘူး။ ပုံထဲမှာပါသလို Storage ကို Hex Editor နဲ့ဖတ်ကြည့်မယ်ဆိုရင် 0 တွေပဲရှိလို့ SSD ထဲမှာ Data တွေမရှိဘူးလို့ ထင်စရာ ရှိပါတယ်။ ဒါပေမဲ့

Wear Leveling/ Garbage Collection / Data Overwritten မဖြစ်ခင်အချိန် အထိ အချက်အလက်တွေက Flash Memory ထဲမှာရှိနေပါတယ်။

Flash Translation Layer (FTL) အထိ မဖတ်နိုင်တဲ့အတွက် data မရှိဖူးလို့ ထင်ရ တာပါ။ ဒါပေမဲ့ HEX Editor နဲ့ဖတ်တဲ့အချိန်မှာ SSD ကို Power ပေးလိုက်တဲ့ အတွက် Wear Leveling, Garbage Collection ပြုလုပ်နေတာကြောင့် Data တွေက လုံးဝ ပျက်စီးသွားနိုင်ပါတယ်။အဓိကပြုလုပ်ရမှာကတော့ Power မပေးပဲ JTAG/ ISP/Chip Off တစ်ခုခုကို လုပ်ရမှာဖြစ်ပါတယ်။ Chip Off ကတော့ အချိန်ယူရသလို စျေးလဲ တော်တော်ကြီးပါတယ်။







SSD Forensics Challenges

HDD နေရာမှာ Solid State Drives (SSD) တွေအစားထိုးအသုံးပြုလာခြင်းက Computer Forensics မှာ ကြီးမားတဲ့ပြောင်းလဲခြင်းဖြစ်လာပါတယ်။ SSD ကို Format ပြုလုပ်လိုက်ရင် Format ထဲမှာမှ Quick Format ပြုလုပ်လိုက်ရင်တောင် မိနစ်ပိုင်းအတွင်းမှာ Data တွေပျောက်သွားပြီး ပြန်လည်ပြီး မရယူနိုင်တော့ပါဘူး။ Format ပြုလုပ်နေတုန်း ပါဝါပိတ်လိုက်ရင်တောင် ပါဝါပြန်တက်လာတဲ့အခါ ပျောက်ဆုံးသွားတဲ့ Data တွေကိုပြန်လည်ရယူ ဖို့ခဲယဉ်း ပါတယ်။ ဘာလို့ဒါမျိုး ဖြစ်လာတာလဲဆိုရင်

Wear Leveling

SSD မှာ Data တွေကို Write လုပ်တာက Page တွေမှာဖြစ်ပါတယ်။ ဒါပေမဲ့ Erase လုပ်တဲ့အခါမှာဆိုရင်တော့ Block Level မှာအလုပ်လုပ်ပါတယ်။ SSD မှာ Read and Write လုပ်နိုင်တဲ့ ပမာဏ Program and Erase (P/E) Cycle ရှိပါတယ်။ Ware Leveling လုပ်တယ်ဆိုတာက SSD မှာရှိတဲ့ Block တွေမှာ (P/E) Cycle ညီမျှအောင်လုပ်ပေးတာဖြစ်ပါတယ်။ Ware Leveling မရှိရင် Data တွေကို သိမ်းတဲ့အခါမှာ (P/E) Cycle များတဲ့ Block နေရာတွေမှာပဲ Read, Erased, Modified (Write) လုပ်နေမယ်ဆိုရင် အချိန်လဲကြာနိုင်သလို SSD ရဲ့သက်တမ်းလဲ တိုနိုင်ပါတယ်။ Ware Leveling က Operation System ကနေပြုလုပ်တာမဟုတ်ပဲ SSD Flash Controller ကနေပြုလုပ်တာဖြစ်ပါတယ်။ SSD Nand Flash မှာဆိုရင်

Data က 2 မျိုးရှိပါတယ်။ Static Data နဲ့ Dynamic Data တို့ဖြစ်ပါတယ်။ Static Data က Cold Data လို့ခေါ်တဲ့ မကြာခန အသုံးမပြုတဲ့ Data တွေဖြစ်ပြီး Dynamic Data က Hot Data ဖြစ်တဲ့ Frequently Changing ဖြစ်နေတဲ့ Data တွေဖြစ်ပါတယ်။ ဒါကြောင့် Ware Leveling မှာ သုံးမျိုးရှိပါတယ်။

Dynamic Ware Leveling

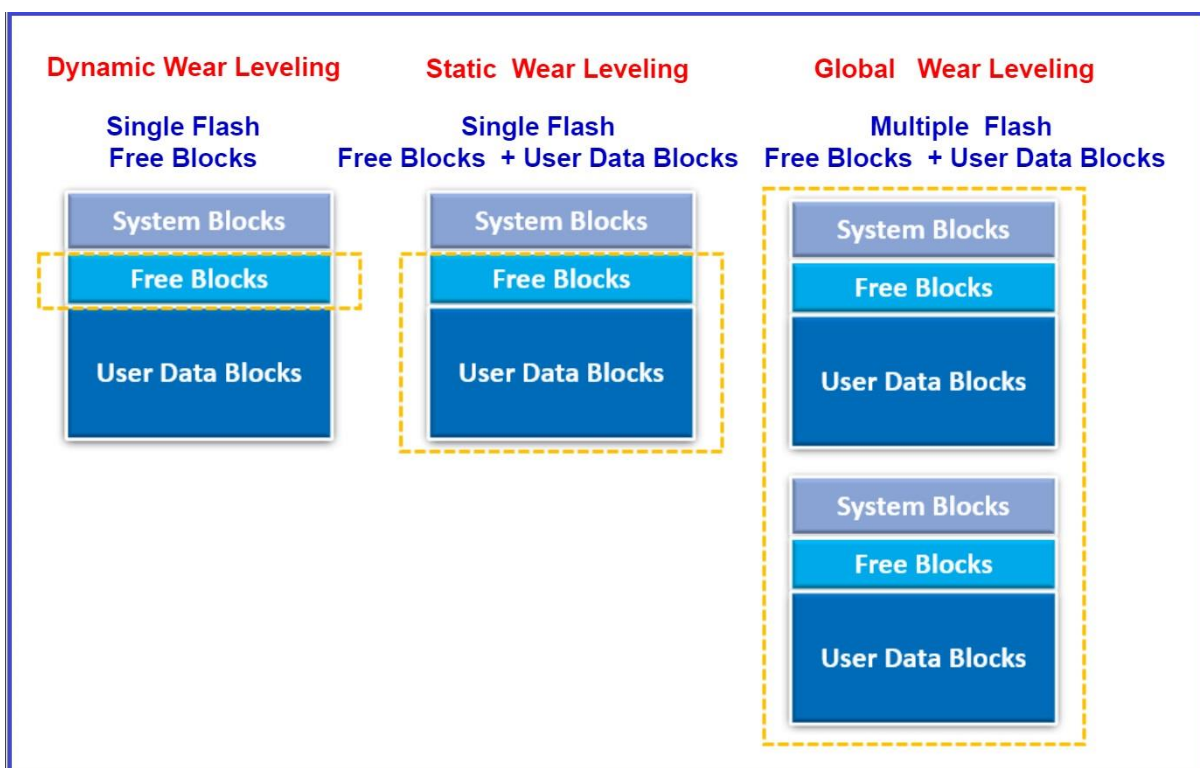
Dynamic Wear Leveling မှာ SSD ထဲကို Dynamic Data တွေကို သိမ်းမယ်ဆိုရင် Free ဖြစ်နေတဲ့ Block နဲ့ (P/E) Cycle (Read/Write) အနည်းဆုံးဖြစ်တဲ့ Block ပေါ်မှာ Data ကိုသိမ်းပါတယ်။ ။ Cold Data တွေရှိတဲ့ Block လိုမျိုး နေရာတွေမပါဝင်တဲ့အတွက် SSD Flash တစ်ခုလုံးစာအတွက် မလုပ်ဆောင်ပါဘူး။ Dynamic Ware Leveling က SSD ကို Performance မြန်စေပြီး Lifspan တိုတောင်းပါတယ်။ Dynamic Wear Leveling အလုပ်လုပ်တာက SSD ထဲမှာ Flash တွေအများရှိတဲ့အထဲက Flash တစ်ခုအတွင်းမှာပဲ ပြုလုပ်တာဖြစ်ပါတယ်။

Static Wear Leveling

Static Wear Leveling မှာတော့ ဥပမာ - SSD ရဲ့ Block တစ်ခုမှာ Static Data/ Cold Data တွေရှိနေမယ် အဲဒီ Data ရှိနေတဲ့ Block ကလဲ (P/E) Cycle (Read/Write) နည်းနေတယ်ဆိုရင် Block ထဲမှာရှိနေတဲ့ Data တွေကို အခြား Block ကိုပြောင်းလိုက်ပါတယ်။ ပြီးရင် Block ကို Free Space လုပ်လိုက်ပြီး Block ကို နောက်တစ်ကြိမ်ပြန်သုံးဖို့အတွက်ထားလိုက်ပါတယ်။ Static Wear Leveling ကတော့ SSD ကို Performance နှေးစေပြီး Lifspan ကို သက်တမ်းရှည်စေပါတယ်။ Static Wear Leveling အလုပ်လုပ်တာက SSD ထဲမှာ Flash တွေအများရှိတဲ့အထဲက Flash တစ်ခုအတွင်းမှာပဲ ပြုလုပ်တာဖြစ်ပါတယ်။

Global Wear Leveling

Global Ware Leveling က Static Ware Leveling နဲ့ဆင်တူပေမဲ့ ကွာခြား ချက်တစ်ခုရှိပါတယ်။ Static Wear Leveling က SSD ထဲမှာ Flash အများကြီး ရှိတဲ့အထဲက Flash တစ်ခုအတွင်းမှာသာ အလုပ်လုပ်ပေမဲ့ Global Wear Leveling ကတော့ SSD ထဲမှာရှိတဲ့ Flash တိုင်းအတွက် အလုပ်လုပ်ပါတယ်။ကျွန်တော်တို့ ပုံကိုကြည့်လိုက်ရင် ပိုပြီး ရှင်းလင်းသွားပါမယ်။



Ware Leveling လုပ်တာကြောင့် Data တွေက Modified လုပ်ရင် Block တစ်ခုထဲမှာမရှိတော့ပဲ Flash သို့မဟုတ် SSD ထဲမှာရှိတဲ့ Flash တွေထဲမှာ ရောက်သွားတဲ့အတွက် အချို့သော Forensics မှာအသုံးဝင်နိုင်တဲ့ အချက်အလက် တွေက SSD တစ်ခုလုံးကို ပြန့်ကျဲကုန်ပါတယ်။ Integrity အတွက် Evidence ကို Hash လုပ်တာမှာလဲ အခက်အခဲရှိလာပါတယ်။ SSD Controller ကနေ အလုပ် လုပ်တာဖြစ်တဲ့အတွက် OS ကနေ SSD ကိုထုတ်ပြီး Write Blocker ခံပြီး Acquire Or Analysis လုပ်မယ်ဆိုရင်လဲ SSD ကို ပါဝါ ပေးတာနဲ့ Ware Leveling က

လုပ်ဆောင်နေမှာဖြစ်ပါတယ်။ SSD ရဲ့ Lifespan တိုးလာအောင်နဲ့ Wear Leveling Porcess လုပ်တာပိုကောင်းလာအောင် SSD ထုတ်တဲ့သူတွေက SSD မှာဖော်ပြထားတဲ့ Storage ပမာဏထက်ပိုပြီး 25 ရာခိုင်နှုန်းပို ပြီးထုတ်လုပ် ထား ပါတယ်။

SSD ထဲမှာ 25 ရာခိုင်နှုန်း ပိုပြီးလုပ်ထားတဲ့ Storage ကို Operation System မှာကြည့်ရင် မပေါ်ပါဘူး။ User ကလဲတိုက်ရိုက်မမြင်နိုင်ပါဘူး။ SSD ထဲက Flash ကိုတိုက်ရိုက် Access လုပ်ဖို့အတွက် သီးသန့်ထုတ်ထားတဲ့ Hardware နဲ့ကြည့်မှသာမြင်တွေ့ရမှာ ဖြစ်ပါတယ်။ SSD ထဲမှာ ဖော်ပြထားတဲ့ ပမာဏထက်ပိုပြီး ရှိနေတဲ့ Storage 25 ရာခိုင်နှုန်းက သာမန်လူတွေအတွက် ပြသာမဟုတ်ပေမဲ့ အချို့သောအစိုးရဌာနတွေကာကွယ်ရေးဌာနတွေအတွက် ပြသာနာဖြစ်လာပါတယ်။ ဘာလို့လဲဆိုရင် သူတို့အသုံးပြုတဲ့ SSD တွေကို အကြောင်းကိစ္စတစ်ခုခုရှိလာရင် Secure Erase လုပ်လို့မရတဲ့အတွက်ဖြစ်ပါတယ်။ 25 ရာခိုင်နှုန်းက Hidden ဖြစ်နေတဲ့အတွက်ကြောင့်ဖြစ်ပါတယ်။

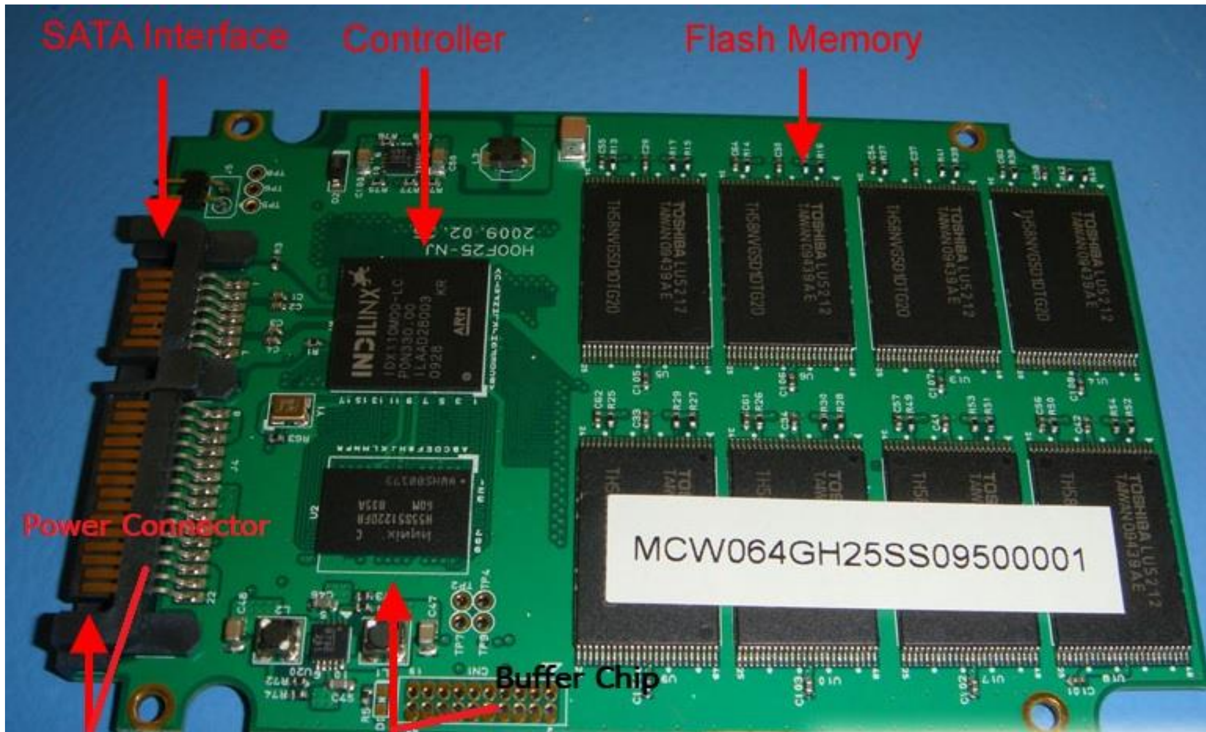
ဒီလိုမျိုးကိစ္စတွေဖြစ်လာတာကြောင့် SSD ထုတ်လုပ်တဲ့သူတွေက SSD မှာ ATA ANSI Specification ဖြစ်တဲ့ ATA Secure Erase (SE) Command ကို SSD ရဲ့ Flash ထဲမှာရှိတဲ့ Dataတွေကို Hardware Level အထိဖျက်ဖို့ ထည့်သွင်းပြုလုပ်လာပါတယ်။ ယေဘူယျအားဖြင့် Software Level Secure Wipe လုပ်တာက Disk ရဲ့အချို့သောနေရာတွေကို မပြုလုပ်နိုင်တဲ့အတွက် ကြောင့်ဖြစ်ပါတယ်။ Disk ထဲမှာရှိတဲ့ data တွေကိုပေါ်ကို Random Bit တွေ Over Write လုပ်လိုက်တာဖြစ်ပါတယ်။ Hardware Level Erase ပြုလုပ်တာကတော့ (System, Reserve, Remapped Area) တွေကိုပါ Secure Erased လုပ်လို့ရပါတယ်။ SSD Controller ကနေ Command ကို Support ပေးလာတာကြောင့် SSD ရဲ့ Flash ထဲမှာရှိတဲ့ Block အားလုံးကို Electronically Erase ပြုလုပ်ပါတယ်။ ဒါကြောင့် Block အားလုံးက အသစ်ဖြစ်သွားပြီး Factory Defaults ဖြစ်သွားပါတယ်။ ပြီးရင် Write လုပ်ထားတဲ့ Data တွေကို SE Command နဲ့ Wipe ပြုလုပ်ဖို့အတွက် Erase

Cycle မလုပ်အပ်ပါဘူး။ SE Command က SSD အတွင်းမှာရှိတဲ့ (System, Reserve, Remapped Area) အပါအဝင် အားလုံးကို Erase ပြုလုပ်နိုင်ပါတယ်။

Wear Leveling Process ဖြစ်တဲ့ Free Block နဲ့ P/E Cycle နည်းတဲ့ Block တွေပေါ်ကိုသာ Data သိမ်းတဲ့အတွက်ကြောင့် SSD Life Span များလာပါတယ်။ ဒါပေမဲ့ Write လုပ်တဲ့ အကြိမ်အရေအတွက်များလာတဲ့အခါမှာ SSD ရဲ့ Flash တွေပေါ်မှာရှိတဲ့ Page File (Blocks Collection) တွေက Dirty ဖြစ်လာပါတယ်။ Dirty ဖြစ်လာတာကြောင့် SSD Write Speed က ပုံမှန်ထက်နှေးလာပါတယ်။ Dirty ဖြစ်လာတဲ့အကြောင်းအရင်းက SSD ထဲမှာရှိတဲ့ Block တွေထဲကို Data Write တဲ့အခါမှာ Data တွေကို Write မလုပ်ခင် Block ကို ပထမဆုံး Erase လုပ်ဖို့လိုအပ်တဲ့အတွက်ကြောင့်ဖြစ်ပါတယ်။ ဒီလိုလုပ်တာက Flash ပါဝင်တဲ့ SSD တိုင်းမှာဖြစ်ပါတယ်။

ဒါလိုဖြစ်စဉ်က အရင်သုံးနေကျ HDD တွေပေါ်မှာ Data ကို Write လုပ်တာနဲ့ ကွာခြားချက်ပဲဖြစ်ပါတယ်။ Block ကို Data Write မလုပ်ခင် Block ကို Erase လုပ်တဲ့ Process ကြောင့် SSD ရဲ့ Performance ကျလာပါတယ်။ Block တွေက Dirty ဖြစ်လာတဲ့အခါ Block တွေပေါ်ကို Data Write လုပ်တဲ့အခါ လိုအပ်တဲ့အချိန်ထက် Write Time ပိုကြာလာပါတယ်။ ဒါကြောင့် Dirty Block တွေကို ရှင်းလင်းဖို့အတွက် SSD Manufacturers တွေကနေ Dirty Block ကိုရှင်း လင်းဖို့အတွက် Garbage Collection ကိုပြုလုပ်လာပါတယ်။ Garbage Collection က Dirty Block တွေကို Background မှာ Erase လုပ်ပေးပြီး Dirty Block တွေကို နောက်တစ်ကြိမ်မှာ Write Time မြန်အောင်ပြုလုပ်ပေးပါတယ်။ ဒီပြဿနာတွေကို ရှင်းလင်းဖို့အတွက် Garbage Collection က Block တွေ မှာ ဘယ် Block မှာ File တွေ OS Information တွေရှိတယ်ဆိုတာနဲ့ မည်သည့် Block တွေက Dirty ဖြစ်နေတယ်ဆိုတာကို မသိပါဘူး။ SSD Controller ကနေ Wear Leveling Process မှာ Block တွေ ပြောင်းလဲတာကို မှတ်သားထားပါတယ်။ SSD ထဲမှာ

ပုံမှန်ပြုလုပ်နေကျ Data တွေ Creating, Writing, Modifying , Deleting လုပ်တာကြောင့်ပဲ Block တွေက Dirty ဖြစ်လာပါတယ်။



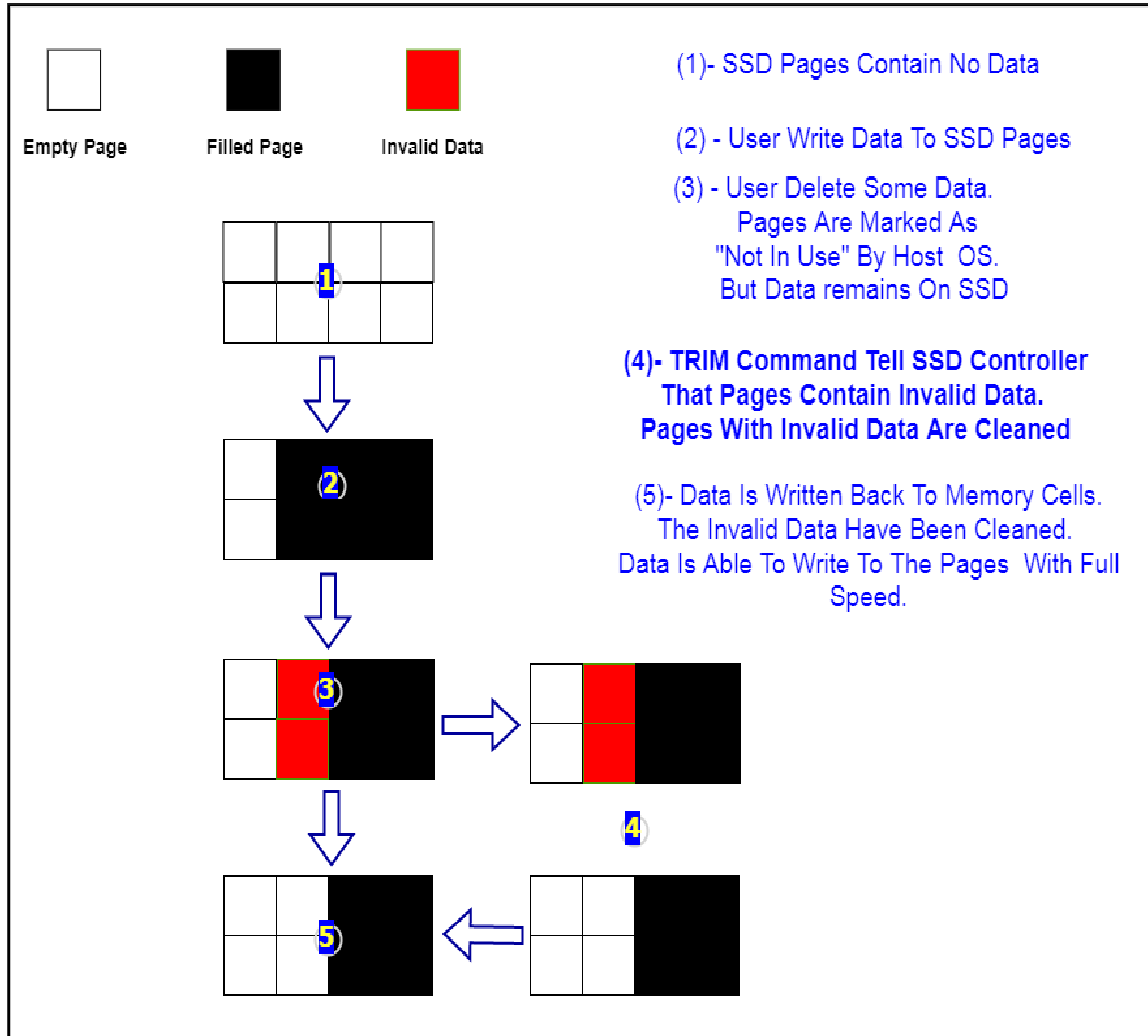
ဒီပြဿနာတွေကို ရှင်းလင်းဖို့အတွက် SSD ထုတ်လုပ်သူတွေက Operation System တွေဖြစ်တဲ့ Windows, Linux, Mac OS X, Etc . တွေကနေ SSD ရဲ့ Controller ကို မည်သည့် File ကတော့ မလိုအပ်တော့ဘူးဆိုတာကို ပြောဖို့အတွက် TRIM Command ကို ထည့်သွင်းလာပါတယ်။ Controller ကေ န Garbage Collector ကို Trim Command ကနေ မလိုအပ်တော့ဘူးပြောတဲ့ File ရှိတဲ့ Block တွေကို Electronically Erase ပြုလုပ်စေပါတယ်။ ဒါမှနောက်တစ်ကြိမ် Write Process လုပ်တဲ့အခါမှာ မြန်ဆန်လာမှာဖြစ်ပါတယ်။

Trim Command --> SSD Controller -- > Garbage Collection

SSD Self-Corrosion

SSD ထဲမှာ ရှိတဲ့ Data တွေကို SSD ကနေ ကိုယ်တိုင်ဖျက်စီးတဲ့ Process ကို SSD Self-Corrosion ပြုလုပ်တယ်လို့ခေါ်ပါတယ်။ Garbage Collection က SSD ရဲ့

Background မှာ အမြဲ Running ပြုလုပ်နေတာကြောင့် ဖျက်ဖို့အတွက် သတ်မှတ်ထားတဲ့ Data တွေကို မိနစ်ပိုင်းအတွင်းမှာ ဖျက်ဆီးလိုက်ပါတယ်။ ဖျက်ဆီးဖို့သတ်မှတ်လိုက်တာနဲ့ မိနစ်ပိုင်းအတွင်း Data တွေကို ဖျက်ဆီးလိုက်တာဖြစ်ပါတယ်။ လက်ရှိ အသုံးပြုနေတဲ့ ကွန်ပျူတာ ထဲကနေ SSD ကိုထုတ်ပြီး အခြား ကွန်ပျူတာမှာသွားတပ်ရင်လဲ Garbage Collection လုပ်တဲ့ Process က ရပ်တန့်သွားမှာ မဟုတ်ပါဘူး။ Write Blocker ကိုကြားထဲမှာခံထားရင်လဲ မရပ်တန့်နိုင်ပါဘူး။ အခုလို SSD ကနေ SSD Self-Corrosion ပြုလုပ်တာကိုတားဆီးဖို့အတွက်ဆိုရင် SSD ထဲမှာရှိတဲ့ Flash တွေကိုခွာပြီး Flash အတွင်းမှာရှိတဲ့ Data တွေကိုဖတ်နိုင်တဲ့ Custom Hardware နဲ့သာပြုလုပ်လို့ရမှာဖြစ်ပါတယ်။ SSD Controller က SSD ထဲမှာရှိတဲ့ Flash တွေကို အဆက်အသွယ်ဖြတ်ပြီး Flash ကို SSD ထဲကနေ ထုတ်ယူပြီး Custom Hardware နဲ့ Flash အတွင်းမှာရှိတဲ့ Data တွေကို ဖတ်တာပါ။ TRIM ကနေ မလိုအပ်တော့တဲ့ Data တွေကို ချက်ချင်းဖျက်ပစ်တယ်လို့ ထင်နိုင်စရာဖြစ်ပါတယ်။ ဒါပေမဲ့ Trim က ကိုယ်တိုင် Erased လုပ်တာမဟုတ်ပါဘူး။ တစ်ကယ်တန်း Erased လုပ်တာက Garbage Collection ကနေပြုလုပ်တာဖြစ်ပါတယ်။ Block ကို Clear လုပ်တဲ့အချိန်ကို Garbage Collection ကနေ နောက်ကွယ်ကနေပြုလုပ်တာကြောင့် SSD ပေါ်ကို Data Write မယ်ဆိုရင် Data Write မလုပ်ခင် Block ကို Erased /Clear လုပ်မဲ့ အချိန်ကို စောင့်စရာမလိုတော့တာကြောင့် SSD Performance ကောင်းလာပါတယ်။



ကျွန်တော်တို့ပုံကိုကြည့်မယ်ဆိုရင် ....

အဆင့် (၁) မှာ SSD Page ထဲမှာ Data တွေမရှိပါဘူး။

အဆင့် (၂) မှာ User ကနေ SSD Page ထဲကို Data တွေထည့်လိုက်ပါတယ်။

အဆင့် (၃) မှာ Page ထဲကနေ Data အချို့ကို ဖျက်လိုက်ပါတယ်။ အဲဒီအချိန်မှာ OS ကနေ အဲဒီ Page ကို Unused အဖြစ်သတ်မှတ်လိုက်ပါတယ်။ ဒါပေမဲ့ Data ကတော့ SSD ထဲမှာ ကျန်နေတုန်းဖြစ်ပါတယ်။

အဆင့် (၄) မှာ Trim Command ကနေ SSD Controller ကို အဲဒီ Page ထဲမှာရှိနေတဲ့ Data က အသုံးမပြုတော့ဘူး ဆိုတာကို လှမ်းပြောပါတယ်။ ပြီးရင် Page အပါအဝင် အသုံးမပြုတော့တဲ့ Data တွေကို Erased လုပ်လိုက်ပါတယ်။

အဆင့် (၅) မှာ SSD ထဲကို Data တွေပြန်ထည့်လိုက်ပါတယ်။ မသုံးတော့တဲ့ Data တွေကိုလဲ ရှင်းလင်းပြီးတဲ့အတွက် နောက်တစ်ခါ Data ကို Write ဖို့အတွက် Full Speed ဖြစ်သွားပါတယ်။

SSD အသုံးပြုထားတဲ့ ကွန်ပျူတာမှာ Trim Command ကို Disable ပြုလုပ်ထားရင်၊ Operation System ကနေ Trim Command ကို Support မလုပ်ရင်၊ SSD ကိုယ်တိုင်မှာ Trim Command မပါခဲ့ရင် SSD ကို သာမန် HDD တွေလိုပဲ Recovery ပြုလုပ်လို့ရပါတယ်။ Trim Command Support ပေးတဲ့ Operation System တွေကိုပုံမှာပြထားပါတယ်။ အသေးစိတ်ကြည့်မယ်ဆိုရင်

Link-1 = https://en.wikipedia.org/wiki/Trim_(computing)

Link-2 = https://wiki.archlinux.org/title/Solid_state_drive

Operating System	Supported since	Notes
DragonFly BSD	May 2011[16]	
FreeBSD	8.1 – July 2010[17]	Support was added at the block device layer in 8.1. Filesystem support was added in FreeBSD 8.3 and FreeBSD 9, beginning with UFS.[18] ZFS trimming support was added in FreeBSD 9.2.[19][20] FreeBSD 10 supports trimming on software RAID configurations.[21]
NetBSD	October 2012[22]	
Linux	2.6.28–25 December 2008[23]	Initial support for discard operations was added for FTL NAND flash devices in 2.6.28. Support for the ATA TRIM command was added in 2.6.33.[24] Not all filesystems make use of trim. Among the filesystems that can issue trim requests automatically are ext4,[25] Btrfs,[26] FAT, GFS2, JFS,[27] XFS,[28] and NTFS-3G. However, in some distributions, this is disabled by default due to performance concerns,[29] in favor of scheduled trimming on supported SSDs.[30] Ext3, NILFS2 and OCFS2 offer ioctls to perform offline trimming. The TRIM specification calls for supporting a list of trim ranges, but as of kernel 3.0 trim is only invoked with a single range that is slower.[31] In many newer Linux distributions, the systemd provides `fstrim.timer` unit, enabling `fstrim.timer` will cause `fstrim.service` to execute weekly.[32]
macOS	10.6.8–23 June 2011[33]	Although the AHCI block device driver gained the ability to display whether a device supports the TRIM operation in 10.6.6 (10J3210),[34] the functionality itself remained inaccessible until 10.6.8, when the TRIM operation was exposed via the IOStorageFamily and filesystem (HFS+) support was added.[citation needed] Until 10.10.4, Mac OS X natively enabled TRIM only for Apple-branded SSDs; third-party utilities are available to enable it for other brands. Old third party TRIM drivers stopped working as of the Yosemite update.[35] Updated drivers now exist that work with OS X Yosemite.[36][37] In Mac OS X update 10.10.4, Apple added a command line utility, trimforce, that can be used to enable TRIM on third-party SSDs.[38]
Microsoft Windows	Windows 7 and Windows Server 2008 R2 – October 2009[39][40]	Windows 7 initially supported TRIM only for drives in the AT Attachment family including Parallel ATA and Serial ATA, and did not support this command for any other devices including Storport PCI-Express SSDs even if the device itself would accept the command.[41] It is confirmed that with native Microsoft drivers the TRIM command works on Windows 7 in AHCI and legacy IDE / ATA Mode.[42] Windows 8 and later Windows operating systems support trim for PCI Express SSDs based on NVMe, and the unmap command which is a full analog of the TRIM command from Serial ATA for devices that use the SCSI driver stack, including USB Attached SCSI Protocol (UASP). Microsoft has released an update for Windows 7 that adds NVM Express support including TRIM for PCIe SSDs.[43][44] TRIM is known to be supported for ReFS and NTFS, both of which implement a DisableDeleteNotify switch for disabling it.[45] Sources disagree on whether TRIM support exists for other filesystems.
OpenSolaris	July 2010[46]	
Android	4.3[47] – 24 July 2013[48]	Runs `fstrim` automatically up to once every 24 hours if the device has been idle for at least an hour and is at least 80% charged (30% if connected to a charger).[47]

ဒီလောက်ဆိုရင် Wear Leveling, Garbage Collection, TRIM Command, SSD Self-Corrosion, အကြောင်းတွေကို အနည်းငယ်သိလောက်ပြီးဖြစ်ပါတယ်။ Trim

Command ကို Support လုပ်တဲ့ Operation System တွေအကြောင်းကိုလဲ ဖော်ပြပြီးဖြစ်ပါတယ်။ SSD Self-Corrosion ကြောင့် Evidence ပျက်တယ်ဆိုတာ User တစ်ယောက်က File, Folder, Volume, Partition ကိုဖျက်မယ် ဆိုရင် Operation System ကနေ Trim ကို On ထားမှ Operation System ကလဲ Support ပေးမှသာ Trim Command ကိုအသုံးပြုလို့ရမှာဖြစ်ပါတယ်။ TRIM Command က Partition Level, Volume Level အထိ အလုပ်လုပ်ပါတယ်။ ဒါကြောင့် Disk Formant, Partition Delete လုပ်တာတွေအထိပါ ပြုလုပ် နိုင်ပါတယ်။

Live ဖြစ်နေတဲ့ System မှာ Trim ON ထားလား OFF ထားလား ကြည့်မယ်ဆိုရင်တော့ Window မှာဆိုရင် fsutil နဲ့ကြည့်နိုင်ပါတယ်။

Check TRIM Status Command In Window Live System

fsutil behavior query disabledeletenotify

Windows TRIM commands Enable = 0

Windows TRIM Commands Disable = 1

Enable Or Disable TRIM Command In Window

Enable = fsutil behavior set disabledeletenotify 0

Disable = fsutil behavior set disabledeletenotify 1

```
:\windows\system32>fsutil behavior query disabledeletenotify
isableDeleteNotify = 1

:\windows\system32>_
```

1 = Windows TRIM Commands - Disabled

```
:\windows\system32>fsutil behavior query disabledeletenotify
isableDeleteNotify = 0

:\windows\system32>
```

0 = Widnow TRIM Command - Enabled

fsutil behavior query disabledeletenotify

Enable Trim - fsutil behavior set disabledeletenotify 0

Disbaled Trim - fsutil behavior set disabledeletenotify 1

၂၀၁၈ တုန်းက ရေးထားတဲ့ POST ပါ။

Hard Disk မှာ Spindle မော်တာကြောင့် လည်ပတ်နေတဲ့ Platter တွေ Platter ပေါ်မှာရှိတဲ့ data တွေသိမ်းထားတဲ့ (track,sector,cluster) တွေကို ဖတ်ဖို့ ရွေ့လျားနေတဲ့ Read / Write Head ပါတဲ့ arm တွေပါရှိပါတယ်။ဒါပေမဲ့ Solid-State Drive (SSD) မှာတော့ လည်ပတ်နေတဲ့ အစိတ်အပိုင်းတွေ မပါဝင်ပါဘူး။ data တွေကို Flash Memory (same as usb stick) ပေါ်မှာ Block အနေနဲ့သာ သိမ်းထားပါတယ်။ လည်ပတ်နေတဲ့ ပစ္စည်းတွေမပါဝင်တဲ့အတွက် vibration ဖြစ်ခြင်းမရှိ၊ အပူထွက်မှုနည်းပါးပြီး HD ထက် အထိအခိုက်ခံတဲ့ အတွက် Solid State Drive လို့ခေါ်ဆိုရခြင်းဖြစ်ပါတယ်။ Data Input-Out နှုန်းမြန်ဆန်ခြင်း၊ လှုပ်ရှားနေတဲ့ အစိတ်အပိုင်းတွေ မပါဝင်တဲ့ အတွက် ထိခိုက်ခံမှုမှာ hard disk ထက်သာလွန်ခြင်း၊ ဆူညံမှုနည်းပါးခြင်း၊ Size သေးငယ်ခြင်း၊ Power အစားသက်သာခြင်း၊ Data ပမာဏ သိုလှောင်မှုများလာပြီး ဈေးနှုန်းလဲ တစ်ဖြည်းဖြည်းသက်သာ လာခြင်းတို့ကြောင့် နောင်တွင်အသုံးပြုမှု ပိုမိုများပြား လာမှာ ဖြစ်ပါတယ်။ SSD မှာ Data တွေကို အဓိက read- write လုပ်တဲ့ Flash Memory ပေါ်မှာပြုလုပ်ခြင်းဖြစ်ပါတယ်။ SSD Flash Memory မှာ သုံးမျိုးရှိပါတယ်။

SSD သက်တမ်းကြာဖို့ TRIM ကိုသုံးနိုင်သလို နောက်ပိုင်း SSD တွေမှာ Wear leveling စနစ်ပါဝင်လာပါတယ်။ SLC (Single-Level Cell) နဲ့ MLC (Multiple-Level Cell) တို့ဖြစ်ပါတယ်။ SLC မှာတော့ Cell တစ်ခုထဲမှာ 1 နဲ့ 0 ထဲကနေ 1 bit ပမာဏကိုသာသိမ်းထားပြီး MCL မှာတော့ Cell တစ်ခုမှာ 2 bit ပမဏ သိမ်းထားနိုင်ပါတယ်။ Triple Leve Cell မှာတော့ Cell တစ်ခုမှာ 3 bit ပမဏ သိမ်းထားနိုင်ပါတယ်။ TLC Cell (SSD) တွေက Storage များပေးမဲ့ Performance နှေးပြီး SSD Life Time လဲနည်းပါးပါတယ်။ အခု user level မှာ အများဆုံ အသုံးပြုနေတာ TLC (SSD) တွေဖြစ်ပါတယ်။ Life time ဆိုတာ SSD မှာ data တွေကို Write လုပ်နိုင်တဲ့ အရည်အတွက် ပမာဏ အပေါ်မူတည်ပြီး သတ်မှတ်တဲ့ SSD ရဲ့သက်တမ်းဖြစ်ပါတယ်။

Controller

Controller Chip ကတော့ SSD ရဲ့ Processor လို့ပြောလို့ရပါတယ်။ အမှန်တစ်ကယ် Data တွေကို သိမ်းထားတဲ့ Flash Memory တွေ နဲ့ SSD ရဲ့ Input-Output Interface ကို ချိတ်ဆက်ပေးပါတယ်။ Error Correction (ECC) အပိုင်းကိုလဲ ဆောင်ရွက်ပေးပါတယ်။ garbage collection, encryption, wear-leveling, , RAISE (Redundant Array of Independent Silicon Elements) အပိုင်းတွေကို ထိန်းညှိပေးပါတယ် ... **Buffer Memory** Buffer Memory Chip ကတော့ သူအသုံးပြုထားတဲ့ Algorithms နဲ့ Type အပေါ်မူတည်ပြီး data တွေကို မြန်ဆန်စွာရရှိစေဖို့ SSD Input-Output Interface နဲ့ SSD Controller ကြားမှာ ဆောင်ရွက်ပေးပါတယ်။ Input-Output Interface နဲ့ Power Connector ကတော့ SSD အမျိုးအစားနဲ့ အသုံးချတဲ့လုပ်ငန်းနဲ့ Device အပေါ်မူတည်ပြီး ကွဲပြားပါတယ်။

Garbage Collection

SSD မှာ Hard Disk ကဲ့သို့ လှုပ်ရှားနေတဲ့ အစိတ်အပိုင်းတွေမပါဝင်တာကြောင့် data တွေကို Read လုပ်ရာမှာရော Write လုပ်ရာမှာရော Hard Disk နဲ့ ကွဲပြားခြား

နားမှုရှိပါတယ်။ (HD မှာ data တွေကို read-write ဘယ်လိုလုပ်တယ် Operation ကနေ Data တွေကို ဖျက်ရင် ဘယ်လိုဖြစ်တတ်ဆိုတာ အရင် Post များတွင် ဖော်ပြပြီးဖြစ်ပါတယ်) SSD Flash Memory မှာ Cell တွေစုစည်ပြီး Page , Page တွေစုစည်းပြီး Block ဆိုပြီးရှိပါတယ်။ data တွေကို သိမ်းရင် Page အဆင့်မှာပဲ သိမ်းထားပေမဲ့ erase လုပ်တဲ့အခါဆိုရင် Block အဆင့်ထိပါ ပြုလုပ်ပါတယ်။ (erase နဲ့ delete မတူပါ) page Size က 2KiB, 4KiB, etc,,, User က data တွေကို အခြား data သိမ်းထားဆဲဖြစ်တဲ့ Block ပေါ်မှာ သိမ်းချင်တယ်ဆိုရင် ရှိနေတဲ့ Block ထဲက data သိမ်းထားတဲ့ Page တွေကို အခြားလွတ်နေတဲ့ Bock ထဲကူးယူ လိုက်ပါတယ်။(ကူးယူပြီးတာနဲ့ Flash Controller က ကူးလိုက်တဲ့ Data ရှိနေတဲ့ Block ရဲ့ logical block address (LBA) ကို အသစ်ထပ်မှတ်လိုက်ပါတယ်။ Data save မဲ့ Page အစုအဝေးဖြစ်တဲ့ Block က Clear ဖြစ်ရင် Erase မလုပ်ပဲ Save ပါတယ်။ Clear မဖြစ်ရင် Erase လုပ်ပြီးမှ Data ကို Save ပါတယ်) **Program/erase cycles (P/E cycles)** ပြီးရင် အရင် Block ထဲက Data တွေကို Erase လုပ်လိုက်ပါတယ်။ ဖျက်ပြီးပြီးဆိုတာနဲ့ နောက် ထပ် Data သိမ်းနိုင်ကြောင်း Flash Controller က Free Block အဖြစ်မှတ်သားထားလိုက်ပါတယ်။ ဒါက Garbage Collection အပိုင်းဖြစ်ပါတယ်။ HD မှာ Bad sector ဖြစ်ရင် သုံးဖို့ Extra Sector တွေပါသလို SSD မှာလဲ Extra Block တွေပါဝင်ပါတယ်။

Wear leveling

Wear leveling ဆိုတာကတော့ SSD တစ်ခုလုံးမှာ ပါတဲ့ Cell တွေကို အကုန် သုံးနိုင် အောင် ပြုလုပ်ပေး တာဖြစ်ပါတယ်။ Program/Erase Cycles (P/E cycles) ကို ထပ်ကာထပ်ကာ အသုံးမပြုပဲ လွတ်နေတဲ့ Block တွေမှာ Data တွေကို Write ပြုလုပ်တာဖြစ်ပါတယ်။

Trim

Trim က Data Write ဖို့ Block ကိုဖျက်တယ် ...ပြီးရင် ပြန် Write တယ်.. Data Write တဲ့ ပမာဏ (File Size)က နည်းလိုက်များလိုက်ဖြစ်လာရင် Cell တွေ Page တွေ Block တွေက ပျံ့ကျဲလာပါတယ်။ ဒါဆိုရင် SSD က လေးလာမယ်။ Trim ကို on ထားရင် လွတ်နေတဲ့ block တွေကိုကြည့်ပြီး data ကိုဖျက်ထားတယ် ဒါမှ နောက်ထပ် Data Save ရင်ပိုမြန်လာမယ်။ Garbage Collection ထပ်ပြီး လုပ်စရာ မလိုအောင်ပါ။ (Garbage Collection, Wear leveling, Trim) ကြောင့်ပဲ SSD ကို Forensics လုပ်ရာမှာ Challenge တွေရှိလာပါတယ်။

SSD မှာအများဆုံးသုံးထားတာက NAND Flash Memory ဖြစ်ပါတယ်။ NOR Flash Memory ကိုတော့ အခုအသုံးပြုနေတဲ့ ဖုန်းများမှာ အသုံးပြုထားပါတယ်။ SSD မှာ Data တွေကို Write - Delete - Rewrite လုပ်ဖို့အတွက် Garbage Collection , (P/E cycles) , Trim တို့ကို သုံးထားတဲ့အတွက် Data Recovery လုပ်ရာမှာ Hard Disk နဲ့ သဘောသဘာဝခြင်းမတူသလို လုပ်ဆောင်ရာမှာ ပိုပြီး ခက်ခဲပါတယ်။ ဥပမာ HD မှာ file အရေအတွက် 50 ရှိရာမှာ recovery ပြန်လုပ်တဲ့ အချိန် File 40 လောက်ပြန်ရနိုင်ပေမဲ့ SSD မှာတော့ 25-30 files လောက်ပဲ ရနိုင်ပါတယ်။ Garbage Collection, (P/E cycles) , Trim အကြောင်းကို သိထားရင် အကောင်းဆုံးပါ။ အသေးထပ်ထပ်စိတ်ရင်တော့ အကောင်းဆုံးပါ Process လုပ် ရာမှာ Knowledge ရှိထားရင်ပိုပြီးအဆင်ပြေပါတယ်။ နောက်ထက် သိထားရမှာ ကတော့ SSD Connector Typeတွေအကြောင်းဖြစ်ပါတယ်။ ဒါမှ Forensics Work Station နဲ့ SSD ကိုချိတ်ဆက်တဲ့အခါ လွယ်ကူမှာ ဖြစ်ပါတယ်။

ဒီလောက်ဆိုရင် SSD ကို Forensics Analysis ပြုလုပ်ရာမှာ သိထားရမဲ့ အခြေခံ ချက်တွေကို နားလည်မယ်လို့ယူဆပါတယ်။ နောက်ထပ် SSD နဲ့ ပတ်သတ်တဲ့ အကြောင်းအရာတွေကိုလဲ ထပ်မံရေးသားဖို့ရှိပါတယ်။ ၂၀၂၃ မှာ Microsoft ကလဲ Boot လုပ်မဲ့ Storage ကို SSD အဖြစ်ပြောင်းလဲမယ်လို့ ကြေငြာထားပါတယ်။ တစ်ကယ်ဖြစ်နိုင် မဖြစ်နိုင်ဆိုတာကတော့ စောင့်ကြည့်ရမှာ ဖြစ်ပါတယ်။

Aung Zaw Myo

SSD Forensics Reference - Yuri Gubanov, Oleg Afonin - Belkasoft Research https://belkasoft.com/

Understanding TRIM, DZAT, and DRAT: Hidden Dangers for SSD Forensics

Window 7 ကနေစပြီးတော့ PC တွေမှာ SSD အသုံးပြုထားရင် Trim က Default အနေနဲ့ On ပါတယ်။ Window 10/11 မှာတော့ အချို့သော Driver Issues ရှိတဲ့ SSD/ NvMe တွေကလွဲရင် Default အနေနဲ့ Trim Enable/ ဖြစ်ပါတယ်။ ပြီးရင် Automatically TRIM လုပ်ပါတယ်။ Trim Enable ဖြစ်/မဖြစ်ကိုတော့ CMD Or Power Shell မှာ fsutil behavior query DisableDeleteNotify ဆိုတဲ့ Command နဲ့စစ်နိုင်ပါတယ်။ (0 = enable , 1 = disable) Trim ကို default အနေနဲ့ Window တွေမှာ On ပေးထားတာက SSD Performance & Lifespan ပိုမိုကောင်းစေဖို့ဖြစ်ပါတယ်။ HDD တွေနဲ့မတူညီတဲ့အချက် SSD တွေမှာ Data Write လုပ်မယ်ဆိုရင် HDD လို Over Write လုပ်လို့မရပဲ အရင်ဆုံ Data Write မဲ့ Block/Page ကို Erase ပြုလုပ်ရပါတယ်။

ဒါပေမဲ့ SSD Controller က Trim အသုံးမပြုနိုင်တဲ့ Controller ဖြစ်နေခဲ့ရင်၊ Internal / External အနေနဲ့သုံးထားတဲ့ SSD မှာ Driver Issues ရှိနေခဲ့ရင်၊ NTFS/ReFS File System အနေနဲ့မဟုတ်ပဲ ကျန်တဲ့ FAT32 File System, Etc.. အနေနဲ့အသုံးပြုထားရင် Trim ကမှန်မှန်ကန်ကန် အလုပ်လုပ်မှာမဟုတ်ပါဘူး။

File တစ်ခုကိုဖျက်လိုက်ရင် ဘယ်လိုဖြစ်မလဲ

Window ကလဲ System မှာ Storage အနေနဲ့ SSD ကိုသုံးပြုထား တယ်ဆိုတာ သိပြီးဆိုတာနဲ့ File တစ်ခုကိုဖျက်လိုက်ရင် Data Read Or Write Command လိုပဲ Trim က Deallocate Command အလုပ်လုပ်ကိုပြုလုပ်ပါတယ်။ TRIM ကို SSD ကနေ Command ပေးတာမဟုတ်ပါဘူး။ Window ကနေ SSD Controller ကို Command ပေးတာဖြစ်ပါတယ်။ ဘယ်အချိန်တွေမှာ OS ကနေ Trim Command ပေးသလဲဆိုရင် File တစ်ခုခုကို

ဖျက်လိုက်တဲ့အခါတိုင်း၊ Partition Format ပြုလုပ်တဲ့အခါတိုင်း၊ Free Space လိုအပ်တဲ့အချိန်တိုင်းမှာ OS ကနေ SSD Controller ကို လက်ရှိမှာ Data သိမ်းထားတဲ့ SSD Block (Logical Block Address ဘယ်လောက်ကနေ ဘယ်လောက်အထိ) ကတော့ မလိုအပ်တော့ဘူး/ ဒီ Block တွေကို မသုံးတော့ဘူး ဖျက်လိုက်ပါဆိုပြီး OS ကနေ SSD Controller ကို Trim Command လှမ်းပြုလုပ်ပါတယ်။

အဲဒီအချိန်မှာ SSD Controller ကနေ Block တွေကို Unused ဒါမှမဟုတ် Free Block တွေအနေနဲ့သတ်မှတ်လိုက်ပါတယ်။ အဲဒီ Data တွေ နောက်ထပ်ဘာဆက်ဖြစ်မလဲဆိုတာက SSD မှာ အသုံးပြုထားတဲ့ Controller, Firmware, SSD Drive Idle time, Background wear-leveling , Garbage Collection ပြုလုပ်တဲ့ ပေါ်မှာမူတည်သွားပါပြီး။ ရှေ့မှာပြောထားတဲ့ အတိုင်းပဲ Data တွေက ရှိခြင်ရှိနိုင်သလို/ မရှိခြင်လဲမရှိတော့ပါဘူး။

OS ကနေ Trim Command ရတာနဲ့ Block တွေကို ချက်ချင်းဖျက်တာရှိသလို၊ မဖျက်ပဲ ဒီ Block တွေကိုတော့ မသုံးတော့ဘူး နောက်မှဖျက်မယ်ဆိုပြီး Unused အနေနဲ့ မှတ်ချင်မှတ်ထားလိုက်ပါမယ်။ အဲဒီ Block ထဲက Data တွေကို နောက်မှ ဖျက်မယ်ဆိုပြီး အခြား Spare Block တွေဆီကိုပို့ချင်လဲပို့လိုက်နိုင်ပါတယ်။ ဒါမှမဟုတ်လဲ လုံးဝမဖျက်တာလဲ ရှိချင်ရှိနိုင်ပါတယ်။

Digital Forensics Analysis မှာ Trim Effect ဘယ်လိုကြုံလာနိုင်မလဲ

OS ကနေ Trim Command ကို SSD Controller ဆီရောက်တာနဲ့ SSD ကနေ အဲဒီ Data တွေကိုအပြီးတိုင်မဖျက်ရင်တောင် SSD Block ထဲမှာရှိနေတဲ့ Data တွေကို SSD Controller ကနေ ပြန်မပြတော့ပါဘူး။ Example Block Number 1 – 10 ကိုဖျက်မယ်ဆိုပြီး OS ကနေ Trim Command ပေးလိုက်တာနဲ့ Block 1 -10 ကနေ Data တွေကို

အပြီးမဖျက်ခဲ့ရင်တောင် Block 1-10 ထဲမှာရှိတဲ့ Data တွေကို SSD Controller ကနေ နောက်တစ်ခါပြန်မပြတော့ပါဘူး။

Block (1 – 10) ထဲက Data တွေကို Computer / Storage Forensics Analysis လုပ်မယ်ဆိုရင် SSD တော်တော်များများက အခုလိုဖော်ပါတယ် -

Undefined

Original Data ပြန်ရချင်ရမယ် ဒါမှမဟုတ် Zero တွေကြည့်ပဲ ပြန်ရမယ်။ (SSD Controller ကနေ Block (1-10) ထဲကနေ Data တွေအစား Zero တွေပဲပြန်ပေးမယ်။)

DRAT (Deterministic Read After TRIM)

(Block 1-10) ထဲမှာ Data ရှိနေရင်တောင် Zero တွေကြည့်ပဲ ပြန်ရမယ်။ (SSD Controller ကနေ Block (1-10) ထဲကနေ Data တွေအစား Zero တွေပဲပြန်ပေးမယ်။)

DZAT (Deterministic Zeros After TRIM)

(Block 1-10) ထဲမှာ Data ရှိနေရင်တောင် Zero တွေကြည့်ပဲ ပြန်ရမယ်။ (OS ကနေ Trim Command ရရချင်း SSD Controller ကနေ Block (1-10) ထဲမှာရှိတဲ့ Data တွေအစား ZERO တွေပဲ ပြန်ပေးပါမယ်။)

Undefined ဖြစ်တဲ့ DATA ရချင်ရမယ် ဒါမှမဟုတ် ZERO တွေပဲပြန်ရမယ်ဆိုတဲ့ SSD တွေက SSD အဟောင်းတွေ၊ Cheap ဖြစ်တဲ့ SSD အမျိုးအစားတွေဖြစ်ပါတယ်။ နောက်ပိုင်း SSD တွေ၊ NVME တွေက DRAT အခြေအနေကိုပဲပြန်ရပါမယ်။ Enterprise Level / RAID Level သုံးတဲ့ SSD တွေက DZAT အခြေအနေကိုပဲပြန်ရပါမယ်။

Wear Leveling

Wear Leveling က SSD Lifespan မကုန်အောင်လုပ်ဆောင်ပေးပါတယ်။ SSD အတွင်း မှာရှိတဲ့ NAND Flash Cell တွေမှာ Program Erase Cycle (P/E) (Write/ Erase) ဆိုတာရှိပါတယ်။ SSD အမျိုးအစားပေါ်မူတည်ပြီး (3000 – 100000) အထိရှိပါတယ်။ အချို့ Cell တွေမှာ Data Read/Write များတဲ့အတွက် သတ်မှတ်ထားတဲ့ Cycle Count ကုန်တာမြန်နိုင်ပါတယ်။ ဒါကြောင့် Wear Leveling က SSD ထဲမှာရှိတဲ့ Cell တွေကိုဖြန့်ပြီး Cycle Count ညီမျှအောင်လုပ်ပေးပါတယ်။ Example ABC DEF ဆိုတဲ့ Cell တွေထဲမှာ ABC က Cycle Count များနေတယ်၊ ABC ထဲမှာ သိမ်းထားတဲ့ Data ကလဲ Hot Data တွေဖြစ်မယ်။ ဒါပေမဲ့ DEF ကတော့ Cycle Count နည်းနေတယ်၊ DEF ထဲမှာ သိမ်းထားတဲ့ Data ကလဲ Cold Data ဖြစ်နေတယ်ဆိုရင် ABC ထဲက Data ကို DEF ထဲကိုပြောင်းပေးလိုက်ပါတယ်။ အဲလိုပြောင်းပေးတာကို Wear Leveling ပြုလုပ်တယ်လို့ခေါ်ပါတယ်။

ABC To DEF ကို Data ပြောင်းပေးတာကို Static Wear Leveling ပြုလုပ်တယ်လို့ခေါ် ပါတယ်။ နောက်တစ်ခုကတော့ Dynamic Wear Leveling ပါ။ Dynamic Wear Leveling ကတော့ ABCDEF ဆိုပြီးရှိတဲ့အထဲမှာမှ ABC က Cycle Count များနေတယ် DEF ကတော့ Cycle Count နည်းနေတယ်ဆိုရင် Data Write ဖို့ရှိလာခဲ့ရင် Controller ကနေ Data ကို Cycle Count များနေတဲ့ ABC အပေါ် Write မပြုလုပ်ပဲ Cycle Count နည်းတဲ့ DEF အပေါ်ကိုပဲ Data Write ပြုလုပ်ပါမယ်။

Garbage Collection

Garbage Collection ကတော့ OS ကနေ ပေးလာတဲ့ Time Command ကိုမှတ်သား ထားပြီး Cell တွေထဲက မလိုအပ်တဲ့ Data တွေကိုဖျက်ပေးပြီး၊ နောက်ထပ် Data Write ခဲ့ရင် အဆင်သင့် ဖြစ်အောင် လုပ်ပေးပါတယ်။ ဒါကြောင့် SSD ကို Read /Write Speed မြန်အောင်လုပ်ပေးပါတယ်။

OS ကနေ Trim Command ရောက်လာတဲ့အခါမှာ မလိုအပ်တဲ့ Cell ထဲမှာရှိတဲ့ Data တွေပိုဖျက်ဖို့အတွက် Garbage Collection အပိုင်းလုပ်ဆောင်ပါလိမ့်မယ်။ Controller ကနေ GC ကိုချက်ချင်းလုပ်ဆောင်တာရှိသလို SSD Busy မဖြစ်တဲ့အချိန် Idle Time မှာ အများဆုံးလုပ် ဆောင်ပါတယ်။ GC ကချက်ချင်းမလုပ်ဆောင်ရင်တောင် SSD Cell ထဲမှာရှိတဲ့ မလိုအပ်တော့တဲ့ Data ကို ဖျက်ဖို့ OS ကနေ Trim Command ကို Controller ကနေရရှိပြီးတာဖြစ်တာကြောင့် Cell အတွင်းက Data ကို GC မလုပ်ရသေးပေမဲ့ အဆိုပါ Cell အတွင်းက Data ကို Forensics Analysis Or Data Recovery လုပ်ရင် Data အစား ZERO တွေကိုပဲ Return ပြန်ပေးပါမယ်။ OS ကနေ Trim Command ရောက်လာပြီးနောက် SSD Controller ကနေ မလိုအပ်တဲ့ Cell ထဲမှာရှိတဲ့ Data တွေကို GC လဲလုပ်ပြီးပြီး။ အဲဒီ Cell ကလဲ Data အသစ်ကိုလက်ခံဖို့အဆင်သင့် ဖြစ်နေပြီးဆိုရင် အရင် Data ပြန်မရနိုင်တော့ပါ။ Wear Leveling ကလဲ SSD Lifespan မကုန်အောင်အမြဲလုပ်နေတာဆိုတော့ GC + Wear Leveling လုပ်ပြီးနောက်မှာ Data ကပြန်မရနိုင်တော့ပါဘူး။

GC ဘယ်အချိန်မှာအများဆုံးလုပ်လဲဆိုရင် Trim Command ရတာနဲ့ ချက်ချင်း လုပ်ချင်လုပ်မယ် SSD Idle ဖြစ်နေတဲ့အချိန်၊ ဒါမှမဟုတ် နောက်တစ်ခါ Computer Boot ပြန်လုပ်တဲ့ အချိန်၊ ဒါမှမဟုတ် SSD Space နည်းနေတဲ့အချိန်မှာလုပ်မယ်။ SSD အမျိုးအစားနဲ့

Controller Firmware အမျိုးအစားအပေါ်မှာမူတည်ပြီး GC ကိုပြုလုပ်မှာဖြစ်ပါတယ်။ အများဆုံးကတော့ Idle ဖြစ်နေတဲ့ အချိန်မှာ အများဆုံးပြုလုပ်ပါတယ်။

အခုကျွန်တော်တို့ SSD ကို အသုံးပြုနေတာက SSD ရဲ့ Standard Mode ကိုအသုံးပြုနေတာ ဖြစ်ပါတယ်။ Data Read မယ် Write မယ်။ အဲတော့ SSD ထဲမှာ GC မပြုလုပ်ရသေးပေမဲ့ Cell အတွင်းမှာ Data ရှိနေရင်တောင်ဖျက်ပြီးသားလို့ OS ကနေ Trim Command ပို့ပြီးပြောထား တာဖြစ်တဲ့အတွက် Controller ကနေ Zero တွေပဲ Return ပြန်ပါမယ်။ Standard Mode Access နဲ့လုပ်လို့မရရင် Factory Mode ကနေ Cell အတွင်းမှာရှိတဲ့ Data ကိုရယူနိုင်ပါတယ်။ GC ချက်ချင်းပြုလုပ်ပြီးရင်တော့ Cell အတွင်းမှာ Data မရှိနိုင်တော့ပါဘူး။ Factory Mode ကို Access ပြုလုပ်ဖို့က Brand ဖြစ်တဲ့ SSD တွေဆိုရင် Company မှာရှိပါတယ်။ နောက်တစ်နည်းကတော့ Storage Forensics Hardware တွေအသုံးပြုဖို့ဖြစ်ပါတယ်။ ဒါပေမဲ့ SSD အားလုံးမရပါဘူး။ Support ပေးတဲ့ SSD အမျိုးအစား Model တွေပဲရပါမယ်။ အပိုင်း (၃) မှာ How To Forensics Analysis အကြောင်းဆက်ရေးသွားပါမယ်။

How To Forensics Analysis (Trim Enable SSD)

- Bootable Forensics OS (OS ကနေ Trim Command ထပ်မပေးနိုင်ရန်အတွက်)
- Cold Method (OS နဲ့ SSD ကိုမချိတ်ဆက်ရင်လဲ SSD ကို Power ပေးတာနဲ့ GC အလုပ်လုပ်တဲ့အတွက် တတ်နိုင်သမျှ SSD Power On Time နည်းအောင် ပြုလုပ်ရန်အတွက်။)